REMARKS

The examiner rejected claim 10 under 35 U.S.C. 112, second paragraph as being indefinite. Applicant has corrected claim 10.

The examiner rejected Claims 1-13, 15, 17-19 and 21 under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards Trapping Wily Intruders in the Large," in view of Katz et al., U.S. Patent 4,575,842.

Claims 1-13, 15, 17-19 and 21 are distinct over Mansfield in view of Katz et al., since the references neither separately nor in combination suggest a port to link the data collector over a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center. The examiner contends that Mansfield in Section 5 and Section 3.1 teaches "communicating the generated statistics over a network to a central control center," and acknowledges that "Mansfield does not disclose utilizing a hardened, redundant network. The examiner relies on Katz to teach "utilizing a hardened, redundant network" to "improve the survivability of the network."

Mansfield neither describes nor suggests the features of a port to link the data collector to a central control center. Rather, Mansfield teaches in section 5:

> The traffic monitoring is carried out using agents which watch all the traffic but process only the suspicious packets. The agents can be accessed, queried and configured using the standard SNMP management protocol. The Security Manager system is alerted on the detection of potential attempts. The Security Manager uses the network configuration information to trap and/or track-down the intruder. The communication between the different Manager's and the agents is carried out using the standard SNMP management protocol.

This teaching does not suggest the control center feature of Applicant's claim 1. At the outset, Mansfield does not suggest that the data collectors deliver the accumulated and collected statistical information about the network packet traffic to the control center as recited in claim 1. Rather, Mansfield teaches to that the "Security Manager system is alerted on the detection of

potential attempts." To the extent that the examiner considers the Security Manager as the central control center, the Security Manager does not receive the data recited in claim 1, but rather is alerted on the detection of potential attempts, suggesting to one of skill that the agents process data looking for attempts. Mansfield confirms this where Mansfield states: "The traffic monitoring is carried out using agents which watch all the traffic but process only the suspicious packets." (Mansfield Section 5.) Moreover, Mansfield also discloses that communications occur between "different Manager's and the agents" using the standard SNMP management protocol. Thus, Mansfield does not suggest a central controller as recited in claim 1.

Katz on the other hand does not suggest a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center. Katz discloses a survivable bus network of multiple buses and network processors. The teaching in Katz is to provide redundancy for normal network traffic in the face of a fault. However, in Katz any one of the redundant bus networks is capable of and would carry the bus traffic. Katz does not suggest a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center.

Applicant also contends that there is no suggestion to combine the teachings of Katz with Mansfield. The examiner's proffered motivation is to "improve the survivability of the network." However, that motivation is of no consequence to either Applicant's claim 1 or to the system alluded to by Mansfield. The examiner has failed to show how Mansfield, which is directed to network intrusion, would be benefited by the teachings of Katz. Katz to the extent that it relates to "attacks" discusses "hostile aircraft "or "communication disruptions" (Col. 7 lines 58-60). In response to an attack Katz reconfigures the bus network (See FIGS. 6 and 7). Accordingly, Katz fails to supply any motivation to modify Mansfield to include a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center. Therefore, claim 1 is allowable over the references.

Claim 2 includes a port to link the data collectors over a redundant network a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets, which as discussed above is not suggested by any combination of Mansfield and Katz.

Claims 3-11 depend directly or indirectly on claim 2 and are allowable with claim 2. Claims 11-13, 15, 17-19 and 21 are also allowable because they each include a similar limitation of a port to link the data collectors over a redundant network a redundant network that does not carry the packet traffic to deliver collected statistical data about the network packets to a central control center.

The examiner rejected Claim 14 under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Katz as applied to claim 13, and further in view of Zait et al., U.S. Patent 6,665,684.

Claim 14 further limits the method of claim 13 by dividing the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter and adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets.

The examiner contends that Mansfield teaches "dividing the traffic flow and using memory spaces to track counts of how many packets a data collector examines for a given parameter (p5, 1st par). ..." In this passage cited by the examiner, Mansfield is merely discussing setting thresholds to see how many related packets are received in order to catch low rate scanner attacks. Mansfield neither describes nor suggests to divide the traffic flow into buckets that track counts of how many packets a data collector or gateway examines for a given parameter. The examiner realized that Mansfield did not suggest "adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets" and instead relied on Zait for this teaching.

However, Zait neither describes nor suggests dividing the traffic flow into buckets nor adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets. Zait is directed to database table partitioning. Zait discusses three

types of partitions "hash-based partitioning and range-based partitioning" (Col. 4 lines 11-12) and a composite partition. (Col. 4 line 10) Zait describes that: "with range-based partitioning, it becomes necessary to add new partitions when newly arriving rows have partition key values that fall outside the ranges of existing partitions." (Col. 4 lines 13-16) Zait describes that: "... all partition key values fall within existing partitions of a hash-partitioned table. However, it may be desirable to add new partitions to a hash-partitioned table, for example, to spread the data over a greater number of devices." (Col. 4 lines 22-26) Zait describes a composite technique of range and hash based partitions.

However, the partitions that Zait discusses are records in a table, e.g., to divide a table of records according to some criteria to make data base management, e.g., improving access to objects (Col. 3 lines 44-45).

Neither Zait nor Mansfield or Katz suggest the desirability of dividing the traffic flow into buckets that track counts of packets examined for a given parameter and adjusting the number of buckets ... by combining several buckets into fewer buckets or dividing a bucket into more buckets. Neither appreciates the problem of an attack that exploits memory space. Zait teaches database management, and is not concerned with attacks that exploit memory space. Mansfield although addressing techniques to address attacks does not recognize the problem of attacks that exploit memory space. Accordingly, claim 14 is allowable over the art, since the combination of references do not suggest the claimed elements and further that there is no suggestion to combine the references.

The examiner rejected Claim 16 under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Katz as applied to claim 15, and further in view of Roesch "Snort-Lightweight Intrusion Detection for Networks."

Claim 16 limits claim 15 by requiring that the layer 3-7 analysis involves monitoring network traffic for unusual levels of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets.

Claim 16 is allowable at least for the reasons discussed in base claim 15. In addition, Roesch describes reassembly of fragments to allow full payload decoding and alerting in the

presence of packet fragments smaller than a predetermined size. Claim 16 recites monitoring for unusual levels of IP fragmentation (that is, more fragmented packets, of any size, than would normally be expect on the network), and detection of fragments with invalid or overlapping fragment offsets. As such, Roesch neither describes nor suggests the features of claim 16.

The examiner rejected Claim 20 under 35 U.S.C. 103(a) as being unpatentable over Mansfield in view of Katz as applied to claim 15, and further in view of Eichstaedt et al., U.S. Patent 6,662,230.

Claim 20 further limits claim 15 by reciting that the layer 3-7 analysis includes monitoring network traffic for an indication of a frequency of re-load requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection. The examiner admits that neither Mansfield nor Katz address this feature, and instead turns to a reference Eichstaedt that pertains to web robots or web-crawlers that obtain documents from a web server.

Initially, applicant notes that claim 20 is directed to a method of collecting data from sampled network traffic, not collecting web pages from a server as taught by Eichstaedt. Eichstaedt teaches to allow a server to limit access to client systems (Col. 6, lines 21-39). Eichstaedt is not concerned with monitoring network traffic for an indication of a frequency of reload requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection. Eichstaedt also does not provide any motivation or solution suitable in the context of Mansfield and Katz or claim 20. While Eichstaedt teaches to limit access to client systems (Col. 6, lines 21-39), such a solution is of no import to an intrusion detection system. Accordingly, whether taken separately or in combination there is no suggestion in Eichstaedt nor the other cited art of monitoring network traffic for an indication of a frequency of reload requests that are sustained at a rate higher than plausible for a human user over a persistent HTTP connection. Therefore, claim 20 is also allowable.

The examiner rejected Claims 1-13 and 21 under 35 U.S.C. 103(a) as being unpatentable over Stallings "Cryptography and Network Security: Principles and Practice," in view of Katz et al., U.S. Patent 4,575,842.

Claims 1-13 and 21 are distinct over Stallings in view of Katz et al., since the references neither separately nor in combination suggest a port to link the data collector over a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center. The examiner contends that Stallings teaches "sampling the network traffic and generating statistics about the network flow," and acknowledges that "Stallings does not disclose utilizing a hardened, redundant network. The examiner relies on Katz to teach "utilizing a hardened, redundant network" to "improve the survivability of the network," the same motivation used by the examiner in the rejection based on Mansfield and Katz.

Applicant contends that Stallings and Katz neither describe nor suggest whether taken together or separately, a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center. Katz discloses a survivable bus network of multiple buses and network processors. The teaching in Katz is to provide redundancy for normal network traffic in the face of a fault. Thus, in the event of a fault another network would carry the network traffic. Katz does not teach to use one network to carry packets and a different redundant network to carry statistical data. In fact, Katz has no relevant teachings related to carrying statistical data. In Katz, any one of the redundant bus networks is capable of and would carry the network traffic. Katz does not suggest a redundant network that does not carry the packet traffic to deliver the accumulated and collected statistical information about the network packet traffic to a central control center.

Applicant also contends that there is no suggestion to combine the teachings of Katz with Stallings. The examiner's proffered motivation is to "improve the survivability of the network." However, that motivation is of no consequence to either Applicant's claim 1 or to the system in Stallings. The examiner has failed to show how Stallings, which is directed to network intrusion, would be benefited by the teachings of Katz. Accordingly, claim 1 is allowable over the references.

Enclosed is a $25 check for excess claim fees and a $60 check for the Petition for Extension of Time fee. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 2/14/05

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21006877.doc